REMARKS/ARGUMENTS

Claims 10-20, 25-27, 30-32, and 35-37 were pending. Upon entry of this amendment, which amends claims 10, 15, 20, 30-32, and 35-37, claims 10-20, 25-27, 30-32, and 35-37 will be pending. Claims 10-20, 30-32, and 35-37 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al. ("Securing Threshold Cryptosystems against Chosen Ciphertext Attack", hereinafter "Shoup") and further in view of Schneier ("Applied Cryptography", hereinafter "Schneier"). Claims 25-27 stand rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Shoup et al. and Schneier, and further in view of Shamir ("How to Share a Secret", hereinafter "Sharmir"). Applicants respectfully request reconsideration of the claims in view of the amendments above and remarks below. Applicants aver that no new matter is introduced in this response.

Examine Interview

Applicants appreciate the interview with the Examiner on April 12, 2006, where claim amendments and the cited prior art were discussed in general.

§103 Rejections

Claims 10, 15, 30-31, 35-36

In the Office Action, the Examiner stated that Shoup in view of Schneir disclose generating keys, encrypting a secret, and distributing the secret to the owners at a custodian computer and receiving k secret owner values from a unique combination of k secret owners then determining a value "c" that is associated with the unique combination and determining the secret S using the value c and the k secret owner values point to page 5 *et seq.* of Shoup and page 527 *et seq.* of Schneier.

Applicants submit claim 10 is allowable over Shoup and Schenier, alone or in combination, as those references fail to disclose or suggest all of the elements of claims 10, 15, 30, 31, 35, and 36. For example, 10, 15, 30-31, and 35-36 partially recite "storing a database of

$\binom{n}{k}$ entries, wherein each entry is associated with a unique combination of the $\binom{n}{k}$ possible combinations of the k secret owners, and wherein a particular entry includes a value, c, that is the product of modulus M of d and the d_i values for i indices that correspond to the particular secret owners present in the unique combination for that particular entry, where c corresponds to modulus M of the product *kdi*".

Shoup and Schneier alone or in combination do not teach storing a database of $\binom{n}{k}$ entries nor do they disclose at least the "*c*" value that represents the product of modulus M of d and the d_i values for i indices that correspond to the particular secret owners present in the unique combination for that particular entry c. The "c" value as taught by Shoup is a cypertext. As claimed, each value c is associated with a unique combination of k secret owners of the n secret owners. Different combinations of k secret owners may return the secret owner pieces. For example, if n=4 and k=3, then different combination of k secret owners may include owners #1, #2, and #3; owners #1, #2, and #4; owners #2, #3, and #4, etc. The value c for each of the unique combinations of k secret owners is stored in the database. As claimed, when k secret owner values from a combination of k secret owners are received, a value c is determined that is associated with unique combination from the database and retrieved. For example, if secret owner values are received from owners #1, #2, and #3, a value c stored in the database associated with that combination is retrieved. The secret S is then determined using the value c and the k secret owner values.

Shoup, Schneier, and Graunke, either alone or in combination, do not disclose or suggest receiving k secret owner values from a combination of k secret owners and retrieving a value c from the database that is associated with that unique combination. The secret S, as claimed, is then determined based on the value c and the k secret owner values. Accordingly, Applicants respectfully request withdrawal of the rejection of claim 10.

Claims 11-14 depend from claim 10 and thus derive patentability at least therefrom. These claims also recite additional novel and non-obvious features. For example, claim 14 recites after the k secret owner pieces are received, the value c is retrieved from the

database and S^c mod N is computed and S' is replaced with S^c mod N. Thus, as recited in claims 11-13, when a secret owner piece is received, S^q mod N is computed and S' is replaced with S^q mod N until the k secret owner pieces have been received and the value c is used to compute S^c mod N to determine the secret S.

Claims 15-20, 25-27, 30-32, and 35-37

Applicants submit claims 15-20, 25-27, 30-32, and 35-37 should be allowable for at least a similar rationale as discussed with respect to claims 10-14. Accordingly, applicants respectfully request withdrawal of the rejections.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

C. Bart Sullivan
Reg. No. 41,516

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
CBS:rgy
60764063 v1